



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

52

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/963,857

09/26/2001

Michael D. Ruehle

42390P11973

1608

8791

7590

04/27/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN  
12400 WILSHIRE BOULEVARD  
SEVENTH FLOOR  
LOS ANGELES, CA 90025-1030

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 04/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/963,857

Applicant(s)

RUEHLE, MICHAEL D.

Examiner

Michael Pyzocha

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 06 September 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 September 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>09262001, 02272004</u> . | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. Claims 1-24 are pending.

***Claim Rejections - 35 USC § 102***

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-6, 8-15, 17-24 are rejected under 35 U.S.C. 102(b) as being anticipated by DeBellis et al (US 6044388).

As per claims 1, 10, 19, and 22 DeBellis et al discloses a hash circuit to receive first and second input values for a current hash stage and to generate an output value from the current hash stage based on the first and second input values (see column 7 lines 8-16); a numerical sequencer coupled to the hash circuit to generate a sequence of numbers during the current hash stage and to provide at least a portion of a current one of the sequence of numbers as the first input value for a subsequent hash stage (see column 6 lines 58-67); a feedback circuit coupled to the hash circuit to provide at least a portion of the output value as the second input value for the

Art Unit: 2137

subsequent hash stage; and a control circuit coupled to the numerical sequencer to stop generating the sequence of numbers upon an occurrence of a first predetermined event and to resume generating the sequence of numbers upon an occurrence of a second predetermined event (see column 7 lines 8-16).

As per claims 2 and 11, DeBellis et al discloses the hash circuit is to receive the first and second input values at a beginning of the current hash stage (see column 7 lines 8-16).

As per claims 3, 12, 20, and 23, DeBellis et al discloses the first predetermined event includes receipt of a request for a pseudo-random number (see column 7 lines 8-40).

As per claims 4-5, 13-14, 21 and 24, DeBellis et al discloses the second predetermined event includes a part of the subsequent hash stage and the part is the beginning (see column 7 lines 8-40).

As per claims 6 and 15, DeBellis et al discloses the numerical sequencer includes a counter (see column 6 lines 58-67 where a timer is a counter).

As per claims 8-9 and 17-18, DeBellis et al discloses said at least a portion of the current one of the sequence of numbers includes predetermined bits of the current one of the sequence of numbers and said at least a portion of the output value

Art Unit: 2137

includes predetermined bits of the output value (see column 7 lines 8-40 where the portion is the whole part).

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 7 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeBellis et al as applied to claims 1 and 10 above, and further in view of Koopman, Jr. (US 5696828).

As per claims 7 and 16, DeBellis et al fails to disclose the numerical sequencer includes a linear feedback shift register.

However, Koopman, Jr. teaches a linear feedback shift register (see column 3 lines 5-22).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Koopman, Jr.'s LFSR in the pseudorandom number generator of DeBellis et al.

Art Unit: 2137

Motivation to do so would have been that a sixty-four (64) bit maximal length LFSR running at a clocked frequency of 1 MHz could be sampled every few seconds to approximate a random number stream and be guaranteed not repeat to itself for 585,000 years (see Koopman, Jr. column 3 lines 5-22).

### ***Conclusion***

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Kaufman et al (US 5483598) discloses a method of encryption using hash functions and feedback.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP



**ANDREW CALDWELL**  
**SUPERVISORY PATENT EXAMINER**